AO 91 (Rev. 11/11) Criminal Complaint (Rev. by USAO on 3/12/20) ☐ Original ☐ Duplicate Original

UNITED STATES DISTRICT COURT

for the

Central District of California

United States of America

v.

Mohamed Hichem EL MABROUK and
Wesley David Adrian DIMOUA-MOUA,

Defendants

Case No. 2:25-mj-00457-DUTY

CRIMINAL COMPLAINT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, the complainant in this case, state that the following is true to the best of my knowledge and belief.

On or about the date(s) of February 1 and 2, 2025, in the county of Los Angeles in the Central District of California, the defendant(s) violated:

Code Section	*Offense Description*
18 U.S.C. §§ 1029(a)(2), 2(a)	Use of unauthorized access devices

This criminal complaint is based on these facts:

Please see attached affidavit.

☒ Continued on the attached sheet.

/s/

Complainant's signature

Jarred Medenwald, Special Agent

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone.

Date: 2/3/2025

Judge's signature

City and state: Los Angeles, California

Hon. Margo A. Rocconi, U.S. Magistrate Judge

Printed name and title

AUSA: Diane Roldán (x6567)

AFFIDAVIT

I, Jarred Medenwald, being duly sworn, declare and state as follows:

I. PURPOSE OF AFFIDAVIT

1. This affidavit is made in support of a criminal complaint against Mohamed Hichem EL MABROUK ("EL MABROUK") and Wesley David Adrian DIMOUA-MOUA ("DIMOUA-MOUA") for violations of 18 U.S.C. § 1029(a)(2) (use of unauthorized access devices).

2. This affidavit is also made in support of an application for a warrant to search the following digital devices (collectively, the "SUBJECT DEVICES"), in the custody of Homeland Security Investigations ("HSI"), in Long Beach, California, as described more fully in Attachment A:

a. A purple Apple iPhone with a black and blue case seized from EL MABROUK's person on February 2, 2025 ("SUBJECT DEVICE 1");

b. A black Apple iPhone bearing IMEI 357334092766783 and seized from DIMOUA-MOUA's person on February 2, 2025 ("SUBJECT DEVICE 2"); and

c. A black Apple iPhone in a clear case seized from DIMOUA-MOUA's person on February 2, 2025 ("SUBJECT DEVICE 3").

3. The requested search warrant seeks authorization to seize evidence, fruits, or instrumentalities of violations of 18 U.S.C. §§ 371 (Conspiracy), 1028A (Aggravated Identity Theft), 1029 (Fraud and Related Activity in Connection with Access Devices), and 1344 (Bank Fraud) (collectively, the "Subject

Offenses"), as described more fully in Attachment B. Attachments A and B are incorporated herein by reference.

4. The facts set forth in this affidavit are based upon my personal observations, my training and experience, and information obtained from various law enforcement personnel and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested complaint and search warrants and does not purport to set forth all of my knowledge of or investigation into this matter. Unless specifically indicated otherwise, all conversations and statements described in this affidavit are related in substance and in part only.

II. SUMMARY OF PROBABLE CAUSE

5. Between January 2024 and January 1, 2025, the California Department of Social Services ("DSS") has detected more than $126.8 million in stolen funds from victim Electronic Benefit Transfer ("EBT") cards. This fraud is from two specific programs known as CalFresh and CalWORKs, which help low-income households pay for housing, food, and other necessary expenses. Many of the fraudulent withdrawals are done at specific ATMs in the Central District of California.

6. On February 2, 2025, law enforcement conducted an operation at several banks to identify potential EBT fraud. As part of the operation, law enforcement conducted surveillance at a U.S. Bank located at 3060 Crenshaw Blvd, Los Angeles, CA 90016 ("Target Bank"), which was identified by DSS as one of the top ATM locations for EBT fraud.

7. Shortly after 6:00 a.m., law enforcement saw EL MABROUK and DIMOUA-MOUA arrive at the Target Bank and conduct multiple transactions. Based on Target Bank and EBT transaction data, EL MABROUK withdrew a total of $2,420 from EBT accounts that did not belong to him using cards encoded with stolen EBT account information. Transaction data showed that at the same time as EL-MABROUK's transactions, DIMOUA-MOUA's attempted three unsuccessful transactions on EBT accounts.

8. U.S. Bank later provided transaction data and surveillance images from the Target Bank for the morning before, February 1, 2025. Based on the data and images, EL MABROUK and DIMOUA-MOUA also conducted unauthorized EBT transactions at the same Target Bank on February 1, 2025, resulting in a total of $25,480 in successful withdrawals.

9. EL MABROUK and DIMOUA-MOUA were arrested and on their persons, law enforcement found SUBJECT DEVICE 1 (on EL MABROUK's person), SUBJECT DEVICE 2 (on DIMOUA-MOUA's person), and SUBJECT DEVICE 3 (on DIMOUA-MOUA's person).

III. BACKGROUND OF AFFIANT

10. I am a Special Agent with the United States Secret Service ("USSS") and have been so employed since May 2016. I am currently assigned to the Homeland Security Investigations ("HSI") El Camino Real Financial Crimes Taskforce in Los Angeles, CA.

11. I have completed criminal investigative training, including the Criminal Investigator Training Program at the Federal Law Enforcement Training Center in Glynco, Georgia, and

the USSS Special Agent Training Course at the James J. Rowley Training Center in Beltsville, Maryland. I have attended multiple advanced and in-service trainings regarding the investigation of cyber-enabled financial crimes, including the Basic Investigation of Computer and Electronic Crimes, Network Intrusion Triage and Response, and training regarding money laundering and asset forfeiture.

12. During my tenure as a Special Agent with USSS, I have investigated and arrested numerous individuals for federal felony offenses including wire fraud, bank fraud, identity theft, money laundering, and access device fraud, among other offenses. During these investigations, I have personally obtained or participated in the execution of several search and seizure warrants for suspect premises, electronic devices and online accounts for the purpose of obtaining digital evidence.

IV. STATEMENT OF PROBABLE CAUSE

13. Based on my review of law enforcement reports, conversations with other law enforcement agents, and my own knowledge of the investigation, I am aware of the following:

A. Regulatory Background of CalFresh and CalWORKs Programs

14. DSS is a government agency that administers several benefit and assistance programs for residents of the state of California. One of the assistance programs administered by DSS is called CalFresh (formerly known as food stamps), which helps low-income households purchase food and household items to meet their nutritional needs. Another assistance program

administered by DSS is called CalWORKs, which helps low-income families with children pay for housing, food, and other necessary expenses.

15. Residents of California that meet the criteria established by the CalFresh or CalWORKs programs can apply online for benefits at www.getcalfresh.org and www.benefitscal.com. Beneficiaries apply for benefits by submitting their income and number of dependents to determine their benefit eligibility.

16. CalFresh and CalWORKs benefits are issued through Electronic Benefit Transfer cards ("EBT cards"). EBT cards are mailed to an address designated by the account holder and function like traditional debit cards to conduct transactions. For example, you can use an EBT card to make a purchase at a grocery or convenient store by swiping the card at a point-of-sale terminal.

17. The EBT cards issued under CalFresh and CalWORKs are assigned specific Bank Identification Numbers ("BIN"). A BIN refers to the first five digits of the account number on a debit or credit card and can be used to identify the issuer of the card, like DSS, which administers the CalFresh and CalWORKs programs.

18. Benefits received through the program are typically disbursed to EBT cardholders by DSS during the early days of each month. Those benefits are deposited directly from DSS into the account of the EBT cardholder.

19. The EBT cardholders can then conduct cash withdrawals at automated teller machines ("ATMs") using a personal identification number ("PIN") established by the card holder. The EBT cardholder presents the card at an ATM, inserts the card into the ATM card reader, and utilizes a PIN to withdraw the funds previously deposited by DSS intended for beneficiaries of the CalFresh or CalWORKs programs.

B. Background on EBT Fraud in the Los Angeles Area and Prior State and Federal Operations

20. Since in or about August 2022, local law enforcement has been working with DSS to investigate a significant increase in unauthorized cash withdrawals utilizing EBT cards. Based on analysis of victim complaints to DSS, victim complaints to local law enforcement, bank records, and surveillance, law enforcement determined that the majority of the unauthorized cash withdrawals were being conducted with cloned cards.

21. A cloned card can be a blank white plastic card or another debit, credit or gift card that contains altered information on the card's magnetic stripe. Based on my training and experience, I know that suspects will often clone cards by taking stolen card information from a victim card's magnetic stripe and re-encode that stolen information onto another card's magnetic stripe. Cloning these cards allows the suspect to use the card and the DSS benefits added on to the account linked to the card for illicit purchases or unauthorized cash withdrawals.

22. On a legitimate debit or credit card, the information contained on the card's magnetic stripe will match the

information embossed on the front of the card. This information includes the account number, expiration date, and cardholder's name, among other information. Whereas on a cloned card, the information contained on the magnetic stripe will not match the information embossed on the front of the card. For example, if a suspect re-encodes victim EBT card information onto a pre-existing gift card's magnetic stripe or a blank white plastic card with a magnetic stripe, the magnetic stripe will be encoded with the EBT card information, but the card itself will still bear the embossed information of the gift card or bear no information if it is a blank white plastic card.

23. Based on my training, experience, and participation in this investigation, I know that the victim card data harvested to clone cards is often obtained from what is colloquially referred to as "skimming activity."

24. The term "skimming" is used to describe activity that involves unlawfully obtaining debit and credit card information by using technological devices to surreptitiously record victim accountholder's debit and credit card numbers and personal identification numbers at, for example, ATMs or point-of-sale terminals. For example, individuals conducting ATM "skimming" may install a skimming device into the card reader of the ATM to record the debit or credit card numbers, as well as a camera or keypad overlay on the ATM keypad to record the associated PIN number. Those individuals will then return to the ATM to collect the card number and PIN information stored on the installed device.

25. As described above, suspects then manufacture cloned and fraudulent debit or credit cards that bear the victim accountholder's account information that was obtained from skimming. Once that information is loaded onto another fraudulent card (e.g., a gift card or blank plastic card), members of the scheme then use that fraudulent card to withdraw cash from the victim accountholder's bank accounts or to make purchases with the victim accountholder's account.

26. In or about September 2022, local law enforcement conducted a surveillance and arrest operation in the Los Angeles, California area. This operation was planned in response to the large number of unauthorized withdrawals occurring at ATMs in the Los Angeles area during a short period of time. Specifically, law enforcement had analyzed fraudulent EBT withdrawal data and noticed a high volume of unauthorized withdrawals on specific dates and times that coincided with the dates when the majority of benefits are disbursed to EBT cardholders.

27. As a result of this operation, local law enforcement established surveillance at select ATMs that were used to conduct a significant volume of EBT fraud. Law enforcement surveilled those ATMs around the dates when benefits had been disbursed, observed suspects that withdrew a high volume of unauthorized withdrawals and that conducted those withdrawals in rapid succession, and arrested multiple individuals believed to be making fraudulent withdrawals of EBT benefits. As a result, law enforcement arrested approximately 16 suspects. All of the

arrested suspects were later determined to be citizens of countries other than the United States who did not have documentation to be lawfully present in the United States. All of the individuals arrested were released from local custody within hours of their arrest and absconded from any future judicial proceedings.

28. In or about February 2023, in response to a further increase in unauthorized cash withdrawals utilizing EBT cards after the local law enforcement September 2022 operation, federal law enforcement conducted a similar surveillance and arrest operation in the Los Angeles, California area. Law enforcement established surveillance around the dates when benefits had been disbursed at select high-volume EBT fraud ATMs. Law enforcement arrested three suspects that withdrew a high volume of unauthorized withdrawals and that conducted those withdrawals in rapid succession. Two of those defendants came to the ATM together, possessed 35 cloned EBT cards at the time of arrest, and later analysis of historic ATM surveillance data showed that they had made more than $190,000 in past attempted fraudulent EBT withdrawals from a single bank since October 2022. One additional defendant possessed 269 cloned EBT cards at the time of arrest, and later analysis of historic ATM surveillance data showed that the defendant had made more than $70,000 in past attempted fraudulent EBT withdrawals from a single bank since January 2023. All three of these defendants were determined to be citizens Romania, who did not have documentation to be lawfully present in the United States. The

three arrested defendants were ordered detained pending trial by the Hon. Karen Stevenson and Hon. Margo A. Rocconi. A federal grand jury returned two indictments against the three defendants for bank fraud, in violation of 18 U.S.C. § 1344; aggravated identity theft, in violation of 18 U.S.C. § 1028A; use of unauthorized access devices, in violation 18 U.S.C. § 1029(a)(2); and possession of unauthorized access devices, in violation of 18 U.S.C. § 1029(a)(3), in 23-CR-0076-FLA and 23-CR-0077-JFW.

29. In or about March 2023, federal law enforcement conducted another surveillance and arrest operation in the Los Angeles, California area. Law enforcement established surveillance around the dates when benefits had been disbursed at select high-volume EBT fraud ATMs. Law enforcement arrested eleven suspects that conducted a high volume of unauthorized transactions and that conducted those transactions in rapid succession. At the time of their arrest, the suspects had in their possession over 400 cloned cards, $120,000 in illicitly obtained funds, and multiple skimming devices.

30. Ten out of the eleven of these defendants were determined to be citizens of Romania, who did not have documentation to be lawfully present in the United States.

C. Background of Current Operation to Combat EBT Fraud

31. The most current data provided by DSS, based in part upon reported fraud by victims, indicates that between January 2024 and January 1, 2025, more than approximately $126.8 million

in cash benefits has been stolen from victim EBT cards throughout California.

32. Of the more than approximately $126.8 million in cash benefits stolen during this year time period, more than approximately $57.9 million has been stolen from victim EBT cards, in the county of Los Angeles alone. The majority of these funds were stolen through unauthorized ATM withdrawals.

33. Between on or about December 1, 2024, and on or about December 31, 2024, according to data from DSS, more than approximately $11.4 million was stolen from victim EBT cards largely through unauthorized ATM withdrawals. Of the approximately $11.4 million stolen from victim EBT cards in the month of December 2024, more than approximately $6.2 million was stolen, mostly through unauthorized ATM withdrawals, in Los Angeles County alone.

34. Based upon my training and experience conducting access device fraud investigations, I know that suspects committing access device fraud schemes will often target particular BINs when harvesting stolen card information collected from skimming devices. Thus, suspects using skimming may target the BIN associated with DSS, in essence, targeting CalFresh and CalWORKs benefits. Moreover, based upon my training and experience, the sheer volume of unauthorized ATM withdrawals occurring during the early days of the month is further indicative that suspects participating in the fraud scheme at issue are targeting EBT cards because benefits are

typically disbursed to EBT cardholders during the early days of each month.

35. Law enforcement has also reviewed ATM surveillance provided by financial institutions that administer EBT accounts that relate to the fraud scheme at issue. During the unauthorized ATM withdrawals, suspects can often be seen holding stacks of cards and conducting withdrawals in quick succession at one ATM. Based upon my training and experience, I know that suspects perpetrating access device fraud schemes will often conduct unauthorized withdrawals using cloned cards in rapid succession at ATMs.

36. Based upon the rapid succession of unauthorized ATM withdrawals being conducted, the fact that the cards being used to conduct the unauthorized cash withdrawals are nearly all cloned EBT cards, and the fact that nearly all of the unauthorized withdrawals are happening during the early days of the month, I believe that suspects participating in the fraud scheme at issue are ostensibly targeting EBT cards.

D. Law Enforcement Observed EL MABROUK & DIMOUA-MOUA Conduct Multiple Rapid ATM Transactions.

37. Based upon the large dollar amount being stolen from victim EBT cards, the number of victims impacted, the concentration of unauthorized ATM withdrawals occurring in particular areas, and the large number of unauthorized ATM withdrawals occurring at singular bank locations, law enforcement conducted a surveillance and arrest operation in February 2025.

38. Based upon my training and experience, I know that as an anti-fraud measure, Cal DSS places an embargo on EBT accounts, such that EBT cardholders are not able to conduct cash withdrawals from their EBT cards until approximately 6:00 a.m., on the morning that their funds load (i.e., the 1st, 2nd, or 3rd of the month, depending on the account).

39. On February 2, 2025, beginning at approximately 5:30 a.m., law enforcement began surveillance on the Target Bank. Law enforcement officers were positioned nearby such that they could see individuals walking up the Target Bank's ATMs and conduct transactions at the ATMs. In addition, law enforcement teams reviewed surveillance images provided by the Target Bank of the ATM transactions from that morning.

40. Based on my review of surveillance images from U.S. Bank and discussions with law enforcement who conducted in-person surveillance that morning, EL MABROUK and DIMOUA-MOUA approached at the Target Bank's ATM terminals together at approximately 6:12 a.m. Law enforcement saw EL MABROUK and DIMOUA-MOUA stand at nearby ATM terminals, where they conducted transactions for approximately five minutes. EL MABROUK and DIMOUA-MOUA both appeared to be conducting several transactions in rapid succession using different cards. Based upon my training and experience, individuals conducting legitimate transactions at ATMs typically conduct a single transaction and do not transition between multiple payment cards rapidly to conduct several transactions in a short period of time.

E. EL MABROUK and DIMOUA-MOUA Had Cloned EBT Cards in Their Possession.

41. Based on my discussions with other law enforcement personnel, review of law enforcement reports and other evidence, and my own knowledge and participation in this investigation, I know that EL MABROUK and DIMOUA-MOUA were subsequently placed under arrest. Law enforcement searched EL MABROUK's and DIMOUA-MOUA's persons. EL MABROUK had approximately 22 cloned access devices on his person. Most of the cloned cards seized from EL MABROUK were gift or prepaid cards, including GreenDot prepaid cards and Vanilla Visa gift cards.

42. Law enforcement analyzed the magnetic stripe of the cloned cards and determined that all of them were cloned cards, encoded with mismatching card numbers. Approximately 21 of the 22 cards seized from EL MABROUK's person were encoded with EBT BINs. The remaining one card was encoded with an unknown BIN at this time. The following is a photograph of the 21 cloned EBT cards seized from EL MABROUK:

43. DIMOUA-MOUA had approximately 11 cloned access devices on his person. Most of the cloned cards seized from DIMOUA-MOUA were gift or prepaid cards, including GreenDot prepaid cards and Vanilla Visa gift cards. Law enforcement analyzed the magnetic stripe of the cloned cards and determined that all of them were cloned cards, encoded with mismatching card numbers and EBT BINs. The following is a photograph of the cloned cards seized from DIMOUA-MOUA:

44. While they were detained at the Target Bank, law enforcement officers heard EL MABROUK and DIMOUA-MOUA speaking to each other in French. Law enforcement later learned that EL MABROUK and DIMOUA-MOUA are both French nationals. Based on my training and experience, and the fact that (1) EL MABROUK and DIMOUA-MOUA arrived to the Target Bank together, (2) they committed unauthorized transactions using cloned CA EBT cards at ATMs next to one another, and (3) they are both French nationals who were speaking to one another in French, I believe EL MABROUK

and DIMOUA-MOUA were likely working together to commit EBT fraud.

F. Transaction Data Revealed That EL MABROUK and DIMOU-MOUA Had Used Stolen EBT Account Data

45. After EL MABROUK and DIMOU-MOUA were arrested, law enforcement obtained additional surveillance images and transaction data from U.S. Bank from February 2, 2025. Based on my review of ATM surveillance stills and logs from U.S. Bank, I saw that EL MABROUK performed three transactions involving EBT card numbers -- all of which matched EBT card numbers encoded on the cloned card seized from EL MABROUK incident to his arrest. Two of those transactions were successful withdrawals totaling $2,420 in financial loss. The remaining one transaction was an attempted withdrawal of $1,900, which was not successful. U.S. Bank ATM surveillance photographs obtained by law enforcement also clearly depicted EL MABROUK at the ATM.

46. Based on my review of ATM surveillance stills and logs from U.S. Bank, I saw DIMOUA-MOUA perform three transactions involving EBT card numbers -- all of which matched EBT card numbers encoded on the cloned card seized from DIMOUA-MOUA incident to his arrest. All three transactions were unsuccessful; in total DIMOUA-MOUA attempted to withdraw $2,760. U.S. Bank ATM surveillance photographs obtained by law enforcement also clearly depicted DIMOUA-MOUA at the ATM.

47. Based on my review of EBT cardholder information obtained from Cal DSS, the CA EBT card ending in 1426 used by EL

MABROUK to withdrawal approximately $1,400 from the Target Bank on February 2, 2025, belongs to victim R.B. of Compton, CA.

48. Based on my review of EBT cardholder information obtained from Cal DSS, the CA EBT card ending in 9476 seized from the person of DIMOUA-MOUA at the Target Bank on February 2, 2025, belongs to victim J.T. of Compton, CA.

G. Law Enforcement Found More EBT Cards and Skimming Devices in EL MABROUK's Car

49. When searching EL MABROUK following his arrest, law enforcement found a car key fob in his pocket. Based on my training and experience and discussions with other law enforcement who specialize in EBT fraud, I know that EBT fraud conspirators often work together. Typically, EBT fraud teams will travel to more than one bank on the same morning to conduct EBT transactions at each bank. They visit multiple banks to avoid being seen standing at any one bank's ATM terminals for too long. The teams typically travel by car because time is of the essence: EBT fraudsters cannot withdraw EBT funds until the embargo lifts at 6:00 a.m., but if they wait too long, the funds may be withdrawn by the legitimate EBT accountholder or by other EBT fraud crews who have stolen the same account information. When EBT fraud teams approach each bank, they typically bring with them only a few of the EBT cards in their possession, so as to avoid attracting attention and to minimize evidence of a crime found on their person. For these reasons and others, based on their training and experience, law enforcement believed that evidence of EBT fraud would likely be found in EL MABROUK

and DIMOUA-MOUA's car. After discovering a car key on EL MABROUK's person, law enforcement used the key to access his vehicle, which was a Land Rover.

50. In the Land Rover, opened with EL MABROUK's key, law enforcement found approximately 20 cloned cards in the center console of the vehicle. Of the approximately 20 cloned cards, approximately 16 were encoded with EBT BINs. Law enforcement also found multiple skimming devices, ATM pin-hole cameras designed to capture victim PIN information, and other skimming contraband in the Land Rover.

H. Surveillance Video Revealed That EL MABROUK and DIMOU-MOUA Had Also Committed EBT Fraud at the Same Bank the Morning Before.

51. After EL MABROUK and DIMOU-MOUA were arrested, law enforcement obtained additional surveillance images and transaction data from U.S. Bank from February 1, 2025, the day before. Based on my review of these surveillance images, EL MABROUK and DIMOU-MOUA were also present at the Target Bank on February 1, 2025, shortly after 6:00 a.m. Based on transaction data from the ATM terminals at that time, EL MABROUK and DIMOU-MOUA used approximately 22 CA EBT cards to attempt to withdrawal approximately $27,720, of which approximately $25,480 was successfully withdrawn.

I. EL MABROUK and DIMOU-MOUA Are French Nationals; DIMOU-MOUA Has Criminal History

52. During processing, it was discovered that both EL MABROUK and DIMOUA-MOUA are both citizens of France.

53. Law enforcement queried EL MABROUK in U.S. Immigration and Customs Enforcement databases and learned that EL MABROUK possesses a valid Visa and employment authorization to be in the U.S.

54. Law enforcement queried DIMOUA-MOUA in U.S. Immigration and Customs Enforcement databases and learned that DIMOUA-MOUA is unlawfully present in the U.S. as a Visa overstay.

55. Law enforcement also learned that DIMOUA-MOUA has been arrested at least five separate times for CA state offenses from 2018 through 2020. These offenses include felony grand theft, grand theft auto, possession of burglary tools, burglary, and identity theft. EL MABROUK has no currently known criminal history.

56. SUBJECT DEVICE 1 was retrieved from EL MABROUK's person following his arrest.

57. SUBJECT DEVICE 2 was retrieved from DIMOUA-MOUA's person following his arrest.

58. SUBJECT DEVICE 3 was retrieved from DIMOUA-MOUA's person following his arrest.

V. TRAINING AND EXPERIENCE REGARDING IDENTITY THEFT CRIMES

59. Based on my training and experience and information obtained from other law enforcement officers who investigate identity theft, I know the following:

a. It is common practice for individuals involved in identity theft, bank fraud, and access device fraud crimes to possess and use multiple digital devices at once. Such digital

devices are often used to facilitate, conduct, and track fraudulent transactions and identity theft. Suspects often use digital devices to perpetrate their crimes due to the relative anonymity gained by conducting financial transactions electronically or over the internet. They often employ digital devices for the purposes, among others, of: (1) applying online for fraudulent credit cards; (2) obtaining or storing personal identification information for the purpose of establishing or modifying fraudulent bank accounts and/or credit card accounts; (3) using fraudulently obtained bank accounts and/or credit card accounts to make purchases, sometimes of further personal information; (4) keeping records of their crimes; (5) researching personal information, such as social security numbers and dates of birth, for potential identity theft victims; and (6) verifying the status of stolen access devices.

b. Oftentimes identity thieves take pictures of items reflecting their stolen identities, including items retrieved from stolen mail or mail matter, with their cellphones.

c. It is also common for identity thieves to keep "profiles" of victims on digital devices. Such "profiles" contain the personal identifying information of victims, such as names, Social Security numbers, dates of birth, driver's license or state identification numbers, alien registration numbers, passport numbers, and employer or taxpayer identification numbers. Identity thieves often keep such information in their cars, storage units, and in their digital devices.

d. It is common for identity thieves, and individuals engaged in bank fraud, access device fraud, and identification document fraud to use equipment and software to print credit and identification cards, to create magnetic strips for credit cards, to use embossing machines to create credit cards, to use laser printers to create checks, and to use magnetic card readers to read and re-encode credit cards. These types of devices are routinely kept where the person will have easy access to such devices, such as on their person or in their cars or homes or storage units. Software relevant to such schemes can also often be found on digital devices, such as computers.

e. Based on my training and experience, I know that individuals who participate in identity theft, bank fraud, and access device fraud schemes often have co-conspirators, and often maintain telephone numbers, email addresses, and other contact information and communications involving their co-conspirators in order to conduct their business. Oftentimes, they do so on their digital devices. Suspects often use their digital devices to communicate with co-conspirators by phone, text, email, and social media, including sending photos. Suspects may also have paper copies of such records, which they may keep on their person or in their cars, homes, or storage units.

f. Individuals engaged in mail and identity theft often use multiple digital devices, which they may keep on their person or in their cars or homes.

VI. TRAINING AND EXPERIENCE ON DIGITAL DEVICES[1]

60. Based on my training, experience, and information from those involved in the forensic examination of digital devices, I know that the following electronic evidence, inter alia, is often retrievable from digital devices:

a. Forensic methods may uncover electronic files or remnants of such files months or even years after the files have been downloaded, deleted, or viewed via the Internet. Normally, when a person deletes a file on a computer, the data contained in the file does not disappear; rather, the data remain on the hard drive until overwritten by new data, which may only occur after a long period of time. Similarly, files viewed on the Internet are often automatically downloaded into a temporary directory or cache that are only overwritten as they are replaced with more recently downloaded or viewed content and may also be recoverable months or years later.

b. Digital devices often contain electronic evidence related to a crime, the device's user, or the existence of evidence in other locations, such as, how the device has been used, what it has been used for, who has used it, and who has been responsible for creating or maintaining records, documents,

[1] As used herein, the term "digital device" includes the SUBJECT DEVICE as well as any electronic system or device capable of storing or processing data in digital form, including central processing units; desktop, laptop, notebook, and tablet computers; personal digital assistants; wireless communication devices, such as paging devices, mobile telephones, and smart phones; digital cameras; gaming consoles; peripheral input/output devices, such as keyboards, printers, scanners, monitors, and drives; related communications devices, such as modems, routers, cables, and connections; storage media; and security devices.

programs, applications, and materials on the device. That evidence is often stored in logs and other artifacts that are not kept in places where the user stores files, and in places where the user may be unaware of them. For example, recoverable data can include evidence of deleted or edited files; recently used tasks and processes; online nicknames and passwords in the form of configuration data stored by browser, e-mail, and chat programs; attachment of other devices; times the device was in use; and file creation dates and sequence.

c. The absence of data on a digital device may be evidence of how the device was used, what it was used for, and who used it. For example, showing the absence of certain software on a device may be necessary to rebut a claim that the device was being controlled remotely by such software.

d. Digital device users can also attempt to conceal data by using encryption, steganography, or by using misleading filenames and extensions. Digital devices may also contain "booby traps" that destroy or alter data if certain procedures are not scrupulously followed. Law enforcement continuously develops and acquires new methods of decryption, even for devices or data that cannot currently be decrypted.

61. Based on my training, experience, and information from those involved in the forensic examination of digital devices, I know that it is not always possible to search devices for data during a search of the premises for a number of reasons, including the following:

a. Digital data are particularly vulnerable to inadvertent or intentional modification or destruction. Thus, often a controlled environment with specially trained personnel may be necessary to maintain the integrity of and to conduct a complete and accurate analysis of data on digital devices, which may take substantial time, particularly as to the categories of electronic evidence referenced above. Also, there are now so many types of digital devices and programs that it is difficult to bring to a search site all of the specialized manuals, equipment, and personnel that may be required.

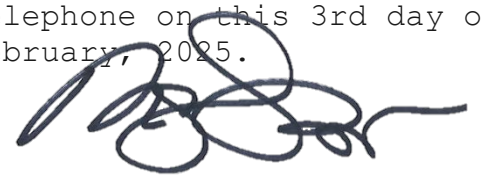
b. Digital devices capable of storing multiple gigabytes are now commonplace. As an example of the amount of data this equates to, one gigabyte can store close to 19,000 average file size (300kb) Word documents, or 614 photos with an average size of 1.5MB.

62. Other than what has been described herein, to my knowledge, the United States has not attempted to obtain this data by other means.

VII. CONCLUSION

63. For all of the reasons described above, there is probable cause to believe that EL MABROUK and DIMOUA-MOUA have each committed violations of 18 U.S.C. § 1029(a)(2) (use of unauthorized access devices). There is also probable cause that the items to be seized described in Attachment B will be found in a search of SUBJECT DEVICE 1, SUBJECT DEVICE 2, and SUBJECT DEVICE 3, as described in Attachment A.

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone on this 3rd day of February, 2025.



THE HONORABLE MARGO A. ROCCONI
UNITED STATES MAGISTRATE JUDGE